#32

Computer & Communications Industry Association

666 Eleventh Street, N.W., Sixth Floor
Washington, D.C. 20001
202.783.0070 Fax 202.783.0534

ENTERED
2/18/97

February 13, 1997

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
Room 2705
14th St. and Pennsylvania Ave., N.W.
Washington, D.C. 20230

Re: Interim Rule on Encryption

Dear Ms. Crowe:

The Computer & Communications Industry Association welcomes the opportunity to offer its comments on the Interim Rule on Encryption published in the Federal Register on December 30, 1996. CCIA is an association of computer and communications industry firms whose members employ over half a million workers and generate annual revenues of nearly 200 billion dollars.

We have a number of serious concerns with the Interim Rule which are set out below.

1. Industrial Policy

Requiring key recovery as a condition of export of encryption products is clearly industrial policy. While the Administration asserts that it is not forcing companies to make key recoverable products, if companies cannot export non-key recoverable items, then there is no real choice involved.

A government-driven process, as opposed to one that is market-driven, runs a considerable risk of being unsustainable. There is not yet any indication that there is a significant market for encryption products with a key recovery system, even if they were not more expensive and even if the uncertainty surrounding the complex legal issues of access and liability could be resolved. With only a limited market, the Administration is requiring U.S. companies to make something that they cannot sell.

As stated in the National Research Council"s seminal study, "Cryptography's Role in Securing the Information Society":

"Imposing a particular solution to the encryption dilemma at this time is likely to have a significant negative impact on the natural market development of applications made possible by new information services and technologies. While the nation may choose to bear these costs in the future, it is particularly unwise to bear them in the absence of a large-scale need that may not arise...."

The study, which we will reference extensively in these comments, was produced by a blue-ribbon panel chaired by Kenneth Dam, Deputy Secretary of State under President Reagan, and included Benjamin Civiletti, former U.S. Attorney General, and Ann Caracristi, Deputy Director of the National Security Agency from 1980 to 1992, and numerous other distinguished individuals from government, industry and academia. While superficially acknowledging the report, the Administration has been far too quick to disregard its recommendations.

The Administration's policy is also unfair to consumers of encryption products. U.S. companies and citizens abroad as well as foreign customers will not be able to get American-made encryption. The government is thereby limiting the choices these entities may have for protecting their security and privacy. Because key recovery-based encryption products are much more expensive than others, the government will be requiring these companies and individuals to spend far more money for a feature that they do not want.

Possibly the most blatantly unfair and futile aspect of the Administration's top-down industrial policy is in the communications sector. There is no consumer demand whatsoever for key recovery in communications. Once an encrypted communication is ended, the participants have no need to be able to recover the substance of what was communicated.

Even the move in the regulations to allow the export of 56-bit encryption products falls short. It conditions a company's ability to export 56-bit encryption for two years on the company's producing a business plan to develop key recoverable encryption products. In addition, the "carrot" of allowing the export of encryption products to the very modest level of 56 bits does not provide our companies with a great deal of relief. The market is demanding more than this level. Foreign companies are developing encryption products at more than this level. There have been threat assessments conducted for individual companies which indicate that 56-bit encryption does not provide sufficient security. It is therefore hard for us to characterize the regulation as a significant relaxation of export controls.

2. Control of Encryption Domestically

The Administration asserts that it is not attempting to control the use or sale of encryption domestically. In a technical legal sense, this is a true statement. However, in a practical sense, it is inaccurate. Unless U.S. companies are willing to

develop two lines of products, one for domestic sale and one for export, the restrictions on exports will act as a de facto restriction on domestic sales as well.

In its study, the National Research Council found that export controls have already affected the domestic market:

"Export controls also have had the effect of reducing the domestic availability of products with strong encryption capabilities. The need for U.S. vendors (especially software vendors) to market their products to an international audience leads many of them to weaken the encryption capabilities of products available to the domestic market. Thus, domestic users face a more limited range of options for strong encryption than they would in the absence of export controls."

3. Key Recovery is Untried

It is indisputable that key recovery is untried, especially on the scale that the Administration is contemplating in its plan. The National Research Council was very clear that key recovery is not sufficiently understood nor ready for widespread implementation: "To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses."

The report supported this recommendation:

"The committee believes that many policy benefits can be gained by an operational exploration of escrowed encryption by the U.S. government, but also that aggressive promotion of the concept is not appropriate at this time for several reasons:

"* The operational complexities of a large-scale infrastructure are significant (especially in an international context of cross-border communications), and a prudent approach to policy would be to develop a base of experience that would guide policy decisions on how escrowed encryption might work on a large scale in practice."

In the Interim Regulation, the Commerce Department recognizes the lack of experience with key recovery:

"Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider requests for eligibility to export key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named, consistent with national security and foreign policy."

Not only is there a profound lack of experience with key recovery, but the challenge of setting up such a system is daunting. Key recovery centers must be established to operate quickly and responsively to numerous requests for information. There is a

significant security risk with imposing such a significant burden on an untried system. The potential is there for keys to be given out by mistake or in response to fraudulent requests. As a result, customers of encryption will be compelled to purchase a feature for which they have little or no desire, is much more expensive, and will create a vulnerability in their system.

4. Key Recovery Lacks Multilateral Consensus

The draft criteria issued by the OECD reference but do not require key recovery. They leave it to the discretion of each country to apply or not apply key recovery as it sees fit. The U.S. Government had sought to make key recovery mandatory but the OECD would not accept that proposal.

Even the proponents of the Administration's encryption policy of mandatory key recovery agree that it will not work absent international agreement. No restrictions on exports are effective unless the countries producing the controlled items are restricting their exports of such items. This is especially true of encryption products which, because of their very nature, are difficult to control under any circumstances. The U.S. Government has come to appreciate the practical limitations on controlling the export of semiconductors. The U.S. Government has also recognized that with a long-distance telephone line and a modem, encrypted software can be sent anywhere in the world.

The potential for undermining the U.S. approach is not theoretical. For example, NTT of Japan has already developed a 128-bit chip. Given the lightening speed of advances in the high-tech arena, it is only a matter of time before many countries are marketing products with such advanced encryption and stronger. Neither the U.S. nor even the OECD countries have a corner on the market of encryption products. Unless the U.S. can gain multilateral and bilateral agreements to restrict exports of all non-key recoverable encryption products, the U.S. policy will not deprive terrorists and criminals of their ability to obtain strong encryption.

5. Competitive Disadvantage for U.S. Companies

The essence of the OECD approach is national discretion. BXA is well aware that for over 40 years under the CoCom structure, "national discretion" meant American business loses. We would lose because the U.S. Government would impose tougher restrictions and implement them more rigorously than our foreign counterparts. The OECD rejection of the U.S. proposal demonstrates that the member countries are not prepared to impose key recovery on their industry. It will be the United States and a few of our close allies who go forward, to the detriment of our companies.

The National Research Council found that:

"Overly restrictive export controls thus increase the likelihood that significant foreign competition will step into a vacuum left by the inability of U.S. vendors to fill a demand for stronger encryption capabilities integrated into general-purpose products." The study found that this stimulation of foreign competition would undermine U.S. national econonic interest by closing the window of opportunity that U.S. companies now have to set important standards and capitalize on their existing competitive advantages.

6. Commercial Espionage

When the keys to decipher the encryption products are held by third parties in foreign countries, the possibility of commercial espionage, a very real concern under existing conditions, would be increased. U.S. Constitutional protections against abuse in obtaining the keys would not apply abroad. It gives little comfort to a company operating in China that the Chinese government would have to go through the legal system to obtain an order allowing it to obtain the key and access to the plain text of the company's marketing plan or research information.

There is also a concern among some companies of the potential of government to government agreements that would apply where a U.S. company doing business abroad was somehow able to keep its encryption keys in the U.S. Under such an arrangement, the U.S. Government would provide the keys to a foreign government upon request of that government.

7. U.S. National Security Interests

It is affirmatively in our national security interest for the U.S. to allow the easy export of higher levels of encryption. As discussed above, the National Research Council found that overly restrictive export controls stimulate the growth of important foreign competitors and thereby undermine traditional national security interests. As the panel stated, "... it is desirable for the U.S. government to keep abreast of the current state of commercially deployed encryption technology, a task that is much more difficult to accomplish when the primary suppliers of such technology are foreign vendors rather than U.S. vendors."

8. Constitutionality of Restrictions

A federal court in northern California has struck down as unconstitutional the State Department's licensing scheme on encryption, Bernstein v. U.S. Department of State (Northern District of California, 1996). The court found that the State Department regulations fail to provide for a time limit on export licensing decisions, fail to provide for judicial review, and do not provide for a duty by the Department of

State to go to court and defend denial of a license. Such regulations are therefore an unconstitutional prior restraint of free speech in violation of the First Amendment.

By virtue of the President's Executive Order of November 1996, jurisdiction over encryption has largely been transferred to the Commerce Department. However, the Commerce Department and the Justice Department have steadfastly refused to allow for judicial review and have refused to require Commerce to go to court to defend denial of a license. As a result, the Commerce regulatory scheme would also fail at least two out of the three criteria established by the court in Bernstein.

Since there is no allowance in these regulations for judicial review or any requirement for the Commerce Department to go to court to defend denial of a license, we would urge that these regulations implement an unconstitutional regulatory scheme and may not go forward in their present form.

9. Law Enforcement

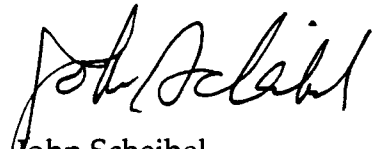
The underlying assumption of the regulations is that by giving the government the ability to read encrypted information, the policy will contribute to law enforcement. Theoretically, the police and other law enforcement agents will be able to obtain information from criminals and others without their knowledge and thereby assist in solving crimes.

However, there are concerns on both sides of the law enforcement issue. By requiring key recovery, the government is creating new targets for attack on a system. It renders the systems of companies, large and small, more vulnerable to breaches of security than they would have otherwise been. Any plan that deprives the private sector of its ability to act in self-defense against criminals that may attack it has got to be suspect. Also, as stated by the National Research Council:

"It is not at all clear that escrowed encryption will be a real solution to the most serious problems that law enforcement authorities will face, because those most likely to have information to conceal will be motivated to exploit technical circumventions of escrowed encryption."

We appreciate the opportunity to provide our comments.

Sincerely,



John Scheibel
Vice President and General Counsel